ATECH IOMART

Service Definition Document

Incident Response Retainer

Contents

Solution Overview

Aims and Objectives

Cyber threats are relentless, and many organisations aren't prepared to act quickly when they strike. The impact of an incident can be severe—financial loss, operational disruption, reputational damage, and regulatory consequences.

While cyber insurance may help with costs, it doesn't contain or resolve the breach.

Our Incident Response Retainer gives you pre-arranged access to certified experts who act fast to investigate, contain, and recover—reducing damage and downtime. With clear plans, a defined team, and round-the-clock availability, it's a practical and cost-effective way to build resilience, meet compliance obligations, and give your business confidence in the face of cyber threats.

Even organisations with strong defences can be caught off guard—having a response plan is essential.

Incident Response Retainer – What is in Scope?

- **Incident Response Hours:** 40 hours per year for DFIR services
- **SLA:** Access to incident responders within 2 hours to immediate assessment and mitigation to stop attacks, recover data, and restore control.
- **Availability:** 24/7/365 hotline access
- **Onboarding**: Team alignment + IR handbook development.
- **Use of Hours:** Management and technical workshops, cyber breach readiness assessments, and IR handbook development.
- **Legal Support**: Available via partner network
- **Additional Hours**: Preferential rates for extra hours if required

Our Approach & What to Expect

From the moment you onboard, we work collaboratively to align teams and define clear response plans tailored to your environment.

Our remote-first mobilisation ensures fast, flexible investigation, while a structured authority model keeps you in control of costs and decisions. When incidents occur, our certified experts conduct forensic analysis to understand the root cause and impact, followed by clear reporting with executive summaries and remediation guidance. You'll be supported throughout the entire lifecycle—from initial triage to full recovery—with consistent communication and expert-led action every step of the way.

Key Features

- CREST CSIR accredited service
- Remote support via zero-configuration remote VPN device and onsite response
- HMG SC cleared consultants
- Thorough onboarding process with integration project
- IASME Cyber Essentials and Cyber Essentials Plus
- Wide experience in public sector networks, including PSN, HSCN, GSi
- CREST Certified Testers in Applications, Infrastructure and Simulated Attack
- 24/7 Incident Response phoneline

Key Benefits

- Cyber Incident Response retainer with defined SLAs
- Guaranteed access to our Incident Response Team during incidents
- End-to-end incident lifecycle coverage
- Quarterly retainer review meetings and dedicated Account Manager
- Complementary incident readiness services are also available
- Services are governed by ISO 9001 and ISO 27001 processes

Scope and Duration

It is anticipated that on commencement of the risk assessment, it will take approximately 4 weeks of elapsed time to complete each of the component pillars, develop report and present.

Assumptions and Pre-requisites

Assumptions

No.	Assumption
1.	All relevant staff are available for calls, meetings, document reviews and workshops (if applicable).
2.	Access to relevant systems is available upon commencement of any work.
3.	Any standards, documentation templates, security policies etc. to be provided to Iomart in advance of the engagement commencing.

Pre-requisites & Engagement Activities

No.	Prerequisite
1.	**It will be necessary for to provide the following in advance of any testing:** • Contact details of personnel to provide support and to resolve any issues with the system(s) under test, should any arise. • IP addresses and hostnames of the targets • Any documents, network Architecture or design details if available. • User credentials for testing the application at each level of authority. Two users at each level per tester. • URLs and other details necessary to reach the targeted application(s). • Whitelisting or similar mechanism to facilitate remote testing of attack IPs.

Data Protection & GDPR

Atech, part of the Iomart Group, is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. Our Data Protection policy sets forth the expected behaviours of Iomart Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to an Iomart Contact (i.e. the Data Subject). Iomart, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in our Data Protection policy (available on request).

Iomart's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all Iomart Employees and Third Parties to share in this commitment.

Iomart uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration of Iomart Entities.
- To provide services to Iomart customers.
- The ongoing administration and management of customer services.
- The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

Each Iomart Entity will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Iomart will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or to take steps at the request of the Data Subject prior to entering a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.

- Processing is necessary to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party.

Why Partner with Atech?

Credentials and Capability

Atech is the one of the UK's most accredited providers of secure hybrid cloud managed services, delivering deep expertise across Microsoft technologies, data protection, and cybersecurity. We hold Microsoft designations for **Modern Work, Security, Infrastructure (Azure)** and are recognised as an **Azure Expert MSP** - a status achieved by only 60 partners globally and 15 in the UK.

As part of the Microsoft AI Cloud Partner Program, we have validated technical capabilities across the full cloud lifecycle. Our inclusion in the **Azure Expert MSP Program** reflects proven excellence in people, processes, and tools, ensuring sustainable, repeatable, and scalable managed services. This means you can rely on a partner that consistently delivers best practice and operational efficiency.

Partnering with us gives you access to over **200 Microsoft cloud specialists**, including **two Microsoft MVPs**, ensuring unparalleled technical depth and experience.

Microsoft Endorsements and Specialisations

We hold multiple Microsoft Solutions Partner designations, including:

- Digital & App Innovation (Azure)
- Data & AI (Azure)
- Business Applications

Figure 1: Microsoft Accreditations

In addition, we have achieved advanced specialisations in areas such as:

- Cloud Security
- Identity and Access Management
- Threat Protection
- Infra & Database Migration
- Azure Virtual Desktop
- Enterprise Application Migration to Azure

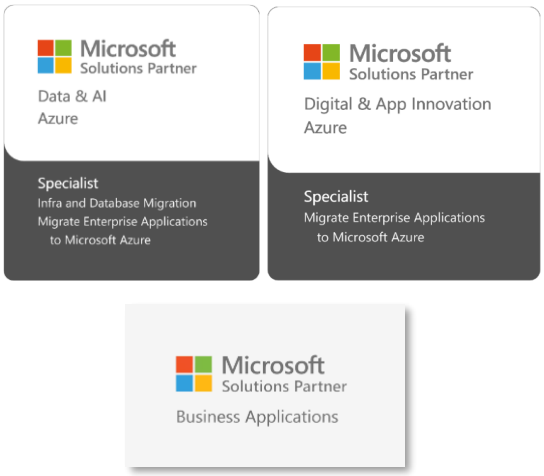

Figure 2: Microsoft Designations

These credentials validate our ability to deliver complex, secure, and innovative solutions aligned to Microsoft best practices.

Security and Compliance

Security is at the heart of our services. Atech is **ISO 27001 certified, Cyber Essentials Plus accredited**, and a member of the **Microsoft Intelligent Security Association (MISA)** – an invitation-only program granting access to Microsoft's top security experts. We also hold **CREST accreditation** and participate in the **Microsoft MSSP Program**, one of only 12 partners in the UK, giving our customers direct benefits such as access to product teams and funded workshops.

Further reinforcing our security leadership:

- **Microsoft Gold Partner Status** alongside **Azure Expert MSP**
- **Microsoft MSSP Program** (1 of only 12 UK partners)
- **Microsoft Fastrack Ready Partner** (1 of only 300 globally)
- **Microsoft XDR status**

These credentials provide you with assurance that security is embedded throughout design, migration, and ongoing management. Combined with our advanced specialisations and industry recognition, they demonstrate our ability to deliver secure, compliant, and future-ready solutions.


ATECH IOMART
6 Atlantic Quay, 55 Robertson Street, Glasgow, G2 8JD